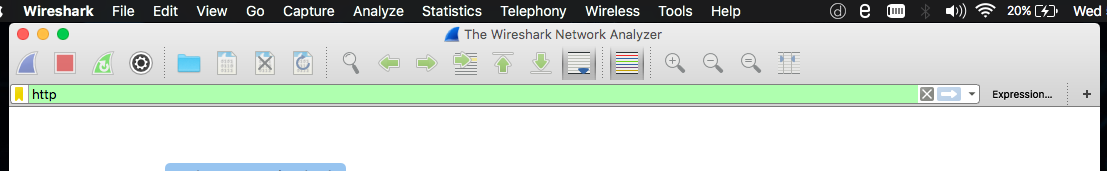
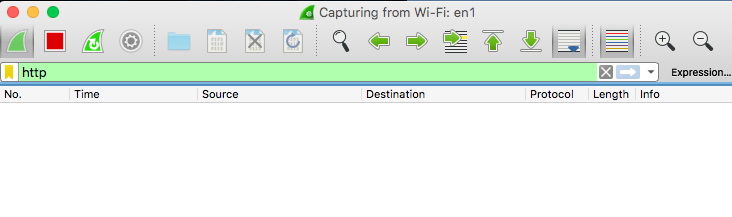
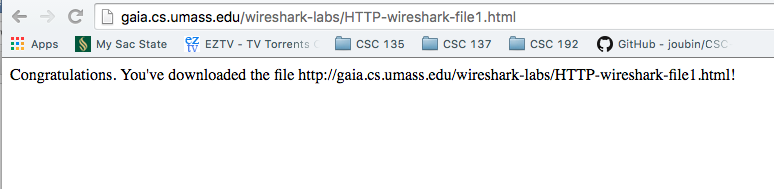
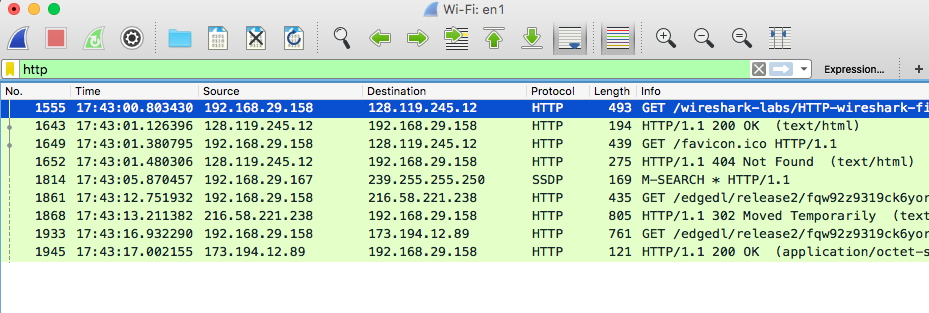
Jaskarn Jagpal

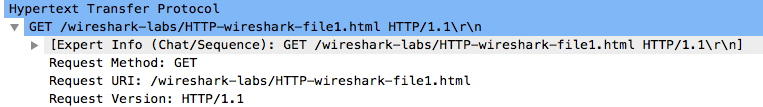
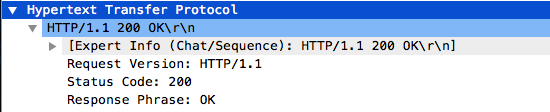
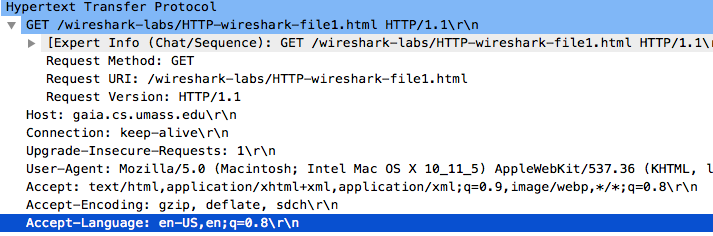
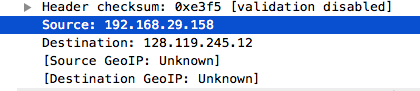
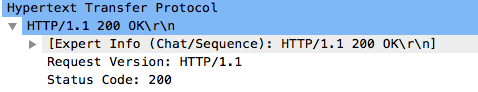
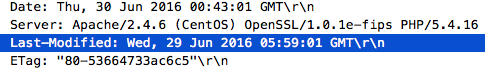
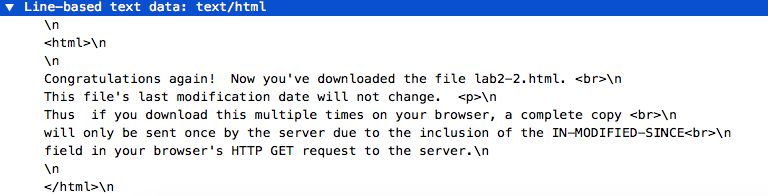
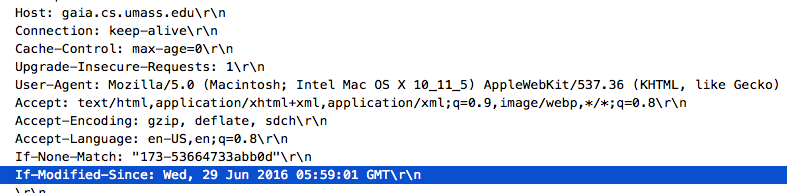
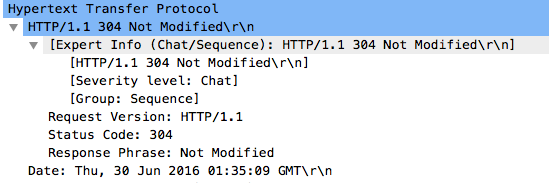
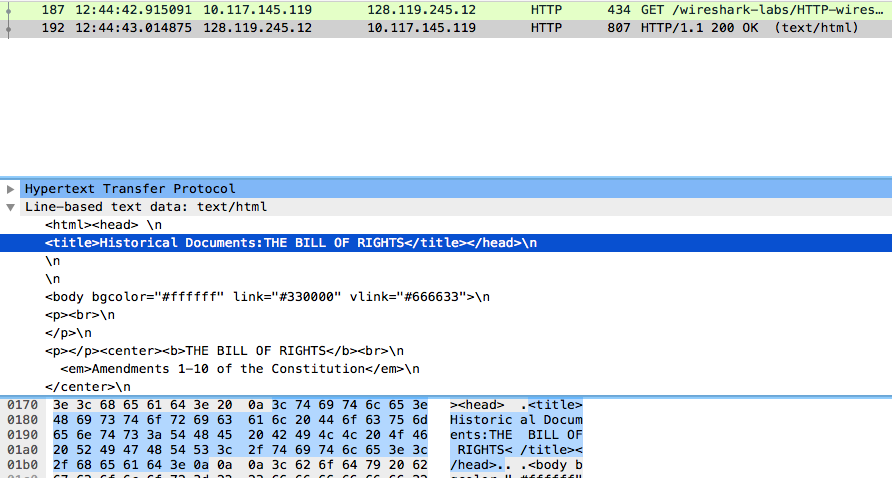
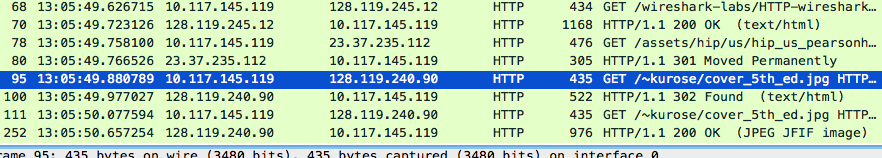
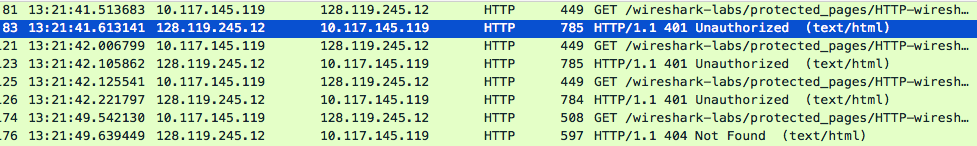
June 29, 2016

CSc 138 T, TH 1240-410

Lab 2 – Wireshark- HTTP

1. Start up your web browser – done.
2. Start up the Wireshark packet sniffer, as described in the introductory lab. Enter “http” in the display-filter-specification windows, so that only captured HTTP messages will be displayed later in the packet-listing window. 
3. Wait a bit more than one minute (we’ll see why shortly), and then begin Wireshark packet capture.
4. Enter the following to your browser http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html Your browser should display the very simple, one-line HTML file.
5. Stop Wireshark packet capture. - done



1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
   1. The browser is running HTTP version 1.1.
   2. The server is running HTTP version 1.1.
2. What languages (if any) does your browser indicate that it can accept to the server?
   1. Accepted language is: en-US, en; q=0.8\r\n
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
   1. IP address of computer is: 192,168.29.158
   2. IP address of gaia.cs.umass.edu server is: 128.119.245.12
4. What is the status code returned from the server to your browser?
   1. The status code returned from the server to the browser is 200.
5. When was the HTML file that you are retrieving last modified at the server?
   1. The HTML file that is being retrieved was last modified at the server on 
6. How many bytes of content are being returned to your browser?
   1. 128 bytes are being returned to the browser. /Users/jaskarnjagpal/Desktop/Screen Shot 2016-06-29 at 6.03.31 PM.png
7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.
   1. No, I do not see any headers within the data that are not displayed in the packet-listing windows.
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?
   1. There is no IF-Modified-Since line in the first HTTP GET request.
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
   1. The server did explicitly return the contents of the file. The content is returned as Line-based text data. 
10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header
    1. An IF-MODIFIED-SINCE header appears in the second HTTP GET request. The information that follows the header is a date and time, Wed, 29 Jun 2016 05:59:01 GMT.
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.
    1. Status code: 304 Not Modified. The file has not been modified, so the text of the file is not returned in the HTTP message. 
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?
    1. Browser sends 1 GET request message.
    2. Packet number 8 in the trace contains the GET message for the bill of rights. 
13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
    1. Packet number 10 contains the status code and phrase associated with the response to the HTTP GET request. Screen%20Shot%202016-06-30%20at%2012.53.09%20PM.png
14. What is the status code and phrase in the response?
    1. Status code: 200
    2. Phrase: OK
15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?
    1. Three packets needed to carry the single HTTP response and the text of the Bill of Rights, packets 10, 11, and 13.
16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
    1. The browser sent 3 HTTP GET messages.
    2. The addresses that the GET requests were sent to are: 128.119.245.12, 23.37.235.112, and 128.119.240.90
17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain
    1. Downloads occurred in parallel, the request for the second image file in packet 20 was made before the OK replay in packet 20 for the first image file was received.
18. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?
    1. Servers response to the initial HTTP GET message is 401 Unauthorized. 
19. When your browser’s sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?
    1. The HTTP GET message should include the Authorization: Basic field and the credentials subfield in the second GET message.